SEP. 29. 2005 3:26PM NO. 0481 P. 3

AF

OIPE IAP08 SEP 29 2005 PATENT & TRADEMARK OFFICE

TRANSMITTAL OF APPEAL BRIEF (Large Entity)

Docket No.
67539/00399

In Re Application Of: LAMBERT, Robert; et al.

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/933,720	08/22/2001	TRUONG, Thanhnga B.	27871	2135	6274

Invention: METHOD AND APPARATUS FOR FINITE FIELD BASIS CONVERSION

COMMISSIONER FOR PATENTS:

Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed on July 29, 2005

The fee for filing this Appeal Brief is: $500.00

☐ A check in the amount of the fee is enclosed.

☒ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 02-2553

☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: Sept. 29 , 2005

John R.S. Orange (Reg. #29,725)
Blake, Cassels & Graydon LLP
Box 25, Commerce Court West
199 Bay Street
Toronto, Ontario M5L 1A9
CANADA
Tel: (416) 863-3164
Fax: (416) 863-2653

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

(Date)

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

10/03/2005 HALI11 00000082 022553 09933720
01 FC:1402 500.00 DA

IN THE UNITED STATES PATENT & TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appl. No.: **09/933,720**

Appellant: **Robert LAMBERT et al.**

Filed: **August 22, 2001**

Title: **METHOD AND APPARATUS FOR FINITE FIELD BASIS CONVERSION**

Art Unit: **2135**

Examiner: **TRUONG, Thanhnga B.**

Docket No.: **67539/00399**

Board of Patent Appeals & Interferences
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

I. INTRODUCTION

This is an appeal from the Final Office Action of the Examiner dated April 29, 2005 rejecting claims 1-27. A Notice of Appeal from the Primary Examiner to the Board of Patent Appeals and Interferences was timely filed with the Office on July 29, 2005.

II. REAL PARTY IN INTEREST

The real party in interest in the present application on appeal is Certicom Corp. The assignment is recorded in the United States Patent and Trademark Office at Reel 012565, Frame 0901 in the present application on appeal, Serial No. 09/933,720.

III. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences known to the Appellant, Appellant's representative or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

IV. STATUS OF CLAIMS

In this application, claims 1-27 are pending and are part of the present appeal. Claims 1-27 have been rejected. Please refer to Appendix A for a complete listing of the claims involved in this appeal.

V. STATUS OF AMENDMENTS

An amendment was filed with the Office subsequent to the final rejection, on September 16, 2005 to place the claims and specification in a better position for consideration. The amendment corrected various typographical errors in the specification and the claims. Amendments were also made to claims 8 and 19 to further characterize certain limitations therein. Appellant submits that the amendment conforms to 37 CFR 1.116.

VI. SUMMARY OF INVENTION

The present invention relates to systems and methods for basis conversion in a cryptographic system.

In one embodiment, either of a pair of correspondents may communicate with an intermediate processor to perform basis conversion for exchanging cryptographic data with the other of the correspondents. Each of the correspondents typically performs cryptographic operations in a different basis, and use the intermediate processor to perform the basis conversion. Such a scheme enables low power devices to exchange data with entities operating in different bases. A method of this embodiment involves a first of the correspondents

transmitting an element such as its public key (represented in terms of its basis) to the intermediate processor. The intermediate processor converts the transmitted element into a second basis representation to produce a converted element, which is forwarded back to the first correspondent. The first entity may then operate on the converted element in a cryptographic operation, such as in computing a signature, for use in exchanging cryptographic data with the second correspondent.

In another embodiment, an exchange of information between a pair of correspondents exchanging cryptographic data and operating in different bases is performed using an intermediate processor. For example, such an embodiment may be used for key exchange. A method of this embodiment involves a first correspondent transmitting an element represented in a first basis, such as its public key, to the intermediate processor; and a second correspondent also transmitting an element represented in a second basis, such as its public key, to the intermediate processor. The intermediate processor then converts the first element into the second basis representation and the second element into the first basis representation to produce first and second converted elements respectively. The first converted element may then be forwarded to the second correspondent and the second converted element to the first correspondent.

As an example, such a method can be used for key exchange between two correspondents, wherein the correspondents may transmit respective public keys that are converted to respective other bases and forwarded to the respective other of the correspondents. Each of the correspondents would then have the pubic key of the other of the correspondents represented in their own basis, and can compute a common key by combining the converted public key with their own private key.

In yet another embodiment, a method is provided for generating a basis independent bit string in a cryptographic system. In the method of this embodiment, a first field element is represented in terms of a first basis. A first function of a first sequence of traces of the first field element is computed, and the first sequence of traces is used as the bit string.

For example, a pair of correspondents operating in different bases, may each have a defined field element represented in terms of its respective basis. The correspondents may then make use of a bit string that is a function of a sequence of traces of the respective field element as a shared secret to perform cryptographic operations.

VII. THE FINAL REJECTION

Claims 1-27 are pending in this application and do not stand allowed. The following discusses each rejection in the order raised in the Final Office Action.

In the Final Office Action dated April 29, 2005, the Examiner rejected claims 12-18 under 35 U.S.C. 102(e) as being anticipated by US Patent No. 5,854,759 to Kaliski, Jr. et al. (hereinafter Kaliski).

The Examiner has stated that the Appellant's arguments with respect to claims 12-18 filed July 14, 2004 have been fully considered but are not persuasive. The Examiner maintains that Kaliski teaches the subject matter of claims 12-18. The Appellant notes that the Appellant's arguments were filed on November 14, 2004 and not July 14, 2004. The Appellant respectfully traverses the Examiner's rejections.

The Examiner has also rejected claims 19-24 under 35 U.S.C. 102(e) as being anticipated by US Patent No. 6,446,205 to Lenstra (hereinafter Lenstra).

The Examiner has also stated that the Appellant's arguments with respect to claims 19-24 have been fully considered but are not persuasive. The Examiner maintains that Lenstra teaches the subject matter of claims 19-24. The Appellant respectfully traverses the Examiner's rejections.

The Examiner has also rejected claims 25-27 under 35 U.S.C. 103(a) as being unpatentable over Lenstra, in view of Kaliski.

The Examiner has also stated that the Appellant's arguments with respect to claims 25-27 have been fully considered but are not persuasive. The Examiner cites *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992); and states that: "In this case, the teaching of Lenstra alone and in combination with Kaliski provide sufficient information and the rejection for claims 19-27 is proper." The Appellant respectfully traverses the Examiner's rejections.

Finally, the Examiner has also rejected claims 1-11 under 35 U.S.C. 103(a) as being unpatentable over Kaliski, and further in view of US Patent No. 5,987,131 to Clapp (hereinafter Clapp) and Lenstra.

The Examiner has stated that the Appellant's arguments with respect to claims 1-11 have been considered but are moot is view of the new ground of rejection indicated above. The Examiner states that "...Kaliski does not explicitly explain in great detail of how Kaliski's cryptographic processor supports the cryptographic operations in multiple bases." The Examiner believes that Clapp and Lenstra teach the missing subject matter not found in Kaliski. The Appellant believes that this new ground of rejection is improper, and in fact contradicts the Examiner's rejection of claim 12 in view of Kaliski. The Appellant respectfully traverses the Examiner's rejections.

VIII. ISSUES

The issues on appeal in this matter are:

1. whether claims 12-18 are unpatentable under 35 U.S.C. 102(e) as being anticipated by Kaliski;
2. whether claims 19-24 are unpatentable under 35 U.S.C. 102(e) as being anticipated by Lenstra;
3. whether claims 25-27 are unpatentable under 35 U.S.C. 103(a) over Lenstra, in view of Kaliski; and
4. whether claims 1-11 are unpatentable under 35 U.S.C. 103(a) over Kaliski, in view of Clapp and Lenstra.

IX. GROUPING OF CLAIMS

The Appellant considers the claims to be separately patentable and as such respectfully submits that the claims do not stand or fall together.

X. APPELLANT'S ARGUMENTS

A. Kaliski does not anticipate claims 12-18

i. Statement of the Law regarding Anticipation under 35 U.S.C. 102

Anticipation can only be established by a single prior art reference: "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987); *Structural Rubber Products Co., v. Park Rubber Co.*, 749 F.2d 7070; 223 U.S.P.Q. 1264 (C.A.F.C. 1984). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The test for anticipation requires that all of the claimed elements must be found in exactly the same situation and united in the same way to perform the same function in a single unit of the prior art. *Studiengesellschaft Kohle, m.b.H. v. Dart Industries., Inc.*, 762 F.2d 724, 726, 220 U.S.P.Q. 841 at 842 (C.A.F.C. 1984). Anticipation cannot be predicated on teachings in a reference that are vague or based on conjecture. *Datascope Corp. v. SMEC Inc.*, 594 F. Supp. 1036; 224 U.S.P.Q. 694, 698 (D.N.J. 1984).

ii. Claim 12

Claim 12 is directed to a method for information exchange between a pair of correspondents exchanging cryptographic data, and operating in different bases. The claimed method recites the following steps:

a) transmitting an element represented in a first basis from a first correspondent to an intermediate processor;

b) transmitting of a second element represented in a second basis from a second correspondent to said intermediate processor;

c) converting the transmitted first element into said second basis representation by said intermediate processor to produce a first converted element;

d) converting the transmitted second element into a first basis representation by said intermediate processor to produce a second converted element;

e) forwarding said first converted element to said second correspondent; and

f) forwarding said second converted element to said first correspondent.

[identifiers added to the above for discussion purposes only]

In the description of the present application, such a method is exemplified as being suitable for key exchange between a pair of correspondents, each of which operates in a different basis. An intermediate processor handles the conversion of, e.g. public keys, to a representation in the other correspondent's basis, and forwards the converted key to the other correspondent to compute, e.g., a common key (see paragraphs [0017] and [0018]). In such an arrangement, only the intermediate processor need perform basis conversion.

iii. <u>The Teachings of Kaliski</u>

Kaliski teaches methods and apparatus for finite field basis conversion. In Figure 1, a basis converter having an externally shifted sequence generator and extractor, takes an internal basis representation A and converts that to an external basis representation B. The apparatus itself operates in accordance with the concepts of basis conversion as described in the Kaliski reference.

An exemplary application of a rotate/extract basis converter is shown in Figures 12-14 of Kaliski, which are primarily relied upon by the Examiner. In Figure 12, a basis converter 150 is shown to have multiple basis converters, namely an import basis converter 152 and a rotate/extract basis converter 154. The basis converter 150 has an input in a first basis

representation and an output in a second basis representation. The internal converters denoted 152 and 154 perform individual conversion operations that are internal to the overall conversion from the input to the output. This includes producing an internal basis representation that exists only between successive operations. Naturally, if two conversion steps are performed, an internal representation would result, however, only for the purpose of bridging the two conversion steps.

Figure 13 extends the application to handling additional basis representations, and includes a finite field arithmetic unit intermediate of the converters 152 and 154. Figure 13 provides only the additional capability of converting an internal representation to an additional representation and vice versa. The primary objective of Kaliski is consistent in this embodiment, namely for providing basis conversion in a resource limited environment. Clearly Kaliski is concerned only with the actual basis conversion algorithms and apparatus therefor. There is nothing suggested by these teachings of how such basis converters should be used. Kaliski is entirely concerned only with algorithms and apparatus for performing efficient basis conversion, and teaches the same.

iv. <u>Appellant's Submissions Regarding Claim 12</u>

As indicated above, the law regarding anticipation requires that each and every element in a claim must be shown in a single reference. Anticipation cannot be predicated on teachings in a reference that are vague or based on conjecture, and must be found in exactly the same situation and united in the same way to perform the same function in a single unit of the prior art. The Examiner believes that Kaliski teaches every element, and thus anticipates claim 12. The Appellant respectfully disagrees.

<u>Preamble and Step a)</u>

In the final rejection, the Examiner first relies on Figure 1 of Kaliski and its accompanying description as teaching the preamble and step a) of claim 12. While referring to Figure 1, Kaliski states *inter alia*, "...basis converter 12...the conversion of an internal basis

representation A to an external basis representation B." This includes having the externally shifted sequence generator 14 compute an internal basis representation of input A.

To reiterate, claim 12 is directed to a method for information exchange between a pair of correspondents exchanging cryptographic data and operating in different bases. Kaliski teaches, in Figure 1, a basis converter having an input and an output. Kaliski does not explicitly teach how or for what the basis converter is used, other than basis conversion itself.

What is inherently required in claim 1 to implement the claimed method is a pair of correspondents who wish to exchange information and an intermediate processor who performs basis conversion to facilitate such transmission. Kaliski does not show nor suggest such an architecture.

Moreover, step a) recited above comprises transmitting a first element represented in a first basis from a first correspondent to an intermediate processor. Figure 1 shows only a basis converter, which could only conceivably be equivalent to the intermediate processor of claim 12 if one were to (for the sake of argument) adopt the Examiner's view (the Appellant however strongly disagrees). If this were the case, it is unclear how the Examiner can contend that Kaliski teaches a step of transmitting a first element from a first correspondent to an intermediate processor, when such a first correspondent and element are neither discussed nor shown.

Kaliski does not teach or even suggest a method for information exchange between a pair of correspondents, let alone the step of transmitting an element represented in a first basis from a first correspondent to an intermediate processor.

<u>Step b)</u>

The Examiner next relies on Figure 13 of Kaliski as reading on step b), which comprises transmitting a second element represented in a second basis from a second correspondent to said intermediate processor. Particularly, the Examiner contends that since the enhanced arithmetic unit in Figure 13 supports operations in both an internal basis and an additional basis and may

include more than one basis converter, the above step is considered to be included in these arithmetic operations.

The system shown in Figure 13 merely extends the functionality of Kaliski's basis converter to handling more than one basis representation. For example, based on what is described in Kaliski, the converter of Figure 13 may convert from the internal representation to an additional representation using the rotate/extract basis converter, and also convert from the additional representation to the internal representation using the import basis converter. Kaliski does not describe in what context the multiple basis representations are used, only that the basis converter shown in Figure 13 accommodates multiple basis representations. Kaliski does not teach transmitting a second element in a second basis from a second correspondent to an intermediate processor. Kaliski only provides a basis converter that can operate in multiple bases.

Again, Kaliski does not show a second correspondent, i.e. a party different to the first, and the intermediary, and therefore, the presence of such a correspondence and the actions he takes is mere conjecture. In fact, the Examiner even states: "...is <u>considered</u> to include.." [emphasis added], further evidencing that Kaliski does not in fact teach such a step but that the Examiner <u>considers</u> that this could be the case.

<u>Steps c) & d)</u>

The Examiner next relies on Figures 12 and 13 and their description in column 16 of Kaliski as reading on steps c) and d) of claim 12 recited above, which comprise converting the first and second elements to first and second converted elements. As discussed above, Kaliski is purely concerned with basis conversion, and Figure 13 extends such basis conversion to handling multiple bases. Steps c) and d) involve the conversion of each element that has been transmitted to the intermediate processor to converted elements. Although Kaliski does not explicitly teach the steps of transmitting the elements to the basis converter, Kaliski does show both an internal representation and an additional representation being converted by the advanced converter 160.

Although Kaliski does teach basis conversion, Kaliski does not teach an intermediate processor performing basis conversion for a pair of correspondents. Therefore, at most, Kaliski could be considered to teach part of step c) or d), but only based on conjecture, which is entirely inappropriate for finding anticipation.

Steps e) & f)

The Examiner has also relied on Figures 12 and 13 of Kaliski as reading on steps e) and f) of claim 12 recited above. These steps comprise forwarding the first converted element to the second correspondent, and forwarding the second converted element to the first correspondent. As discussed above, Kaliski does not teach or even suggest two different correspondents transmitting different elements represented in different bases to an intermediate processor. Kaliski does not in any way teach forwarding converted elements to respective correspondents.

Kaliski teaches a basis converter that takes an input, converts that input, and produces an output in a different basis. Even if, for the sake of argument, one were to take Kaliski's basis converter and implement it in a cryptographic system (which the Appellant stresses Kaliski does not teach), Kaliski still does not provide an intermediary that performs basis conversion, which is also separate from a pair of corresponding entities, nor teach forwarding converted elements to the respective other correspondent. Kaliski could only be considered to have a single entity perform the basis conversion itself, that entity also using and/or sending the element for use in cryptographic operations. This requires that the entity producing or using the element also perform basis conversion, which is what claim 12 completely avoids. Kaliski does not teach the use of basis conversion in the architecture inherently required by claim 12. Kaliski is entirely silent as to how his basis converter could be used for a cryptographic system.

As discussed above, the method recited in claim 12 helps to conserve power since neither of the communicating correspondents need to perform basis conversion, but use an intermediate processor to properly convert elements from the basis representation of the sender to the basis representation of the receiver and vice versa. Such a method may be used for key exchange and the like. In order to complete such an exchange, the intermediate processor forwards the first

converted element to the second correspondent and the second converted element to the first correspondent.

Contrary to the Examiner's view, Kaliski simply does not teach such steps. Kaliski is only concerned with basis conversion itself and in no way teaches any exchange of information that involves "swapping" converted elements, wherein the elements have undergone respective basis conversion operations. Kaliski does not teach an intermediary corresponding with a pair of correspondents, let alone using an intermediary to perform basis conversion for the pair of correspondents as recited in the claim. The Examiner has failed to identify these steps and appears to have relied on a vague extrapolation of the teachings of Kaliski. In fact, the Examiner even states: "Thus it is well- known in the art that these cryptographic operations are applicable to cryptographic and/or Diffie-Hellman key exchange". The Examiner has failed to find all claim elements in exactly the same situation and united in the same way in a single prior art reference, and therefore Kaliski cannot anticipate claim 12.

In view of the foregoing, the Appellant respectfully submits that Kaliski cannot serve as an anticipatory reference for the reference fails to teach every element of Appellant's claim 12.

v. Appellant's Submissions Regarding Claims 13-18

Claims 13-18 are either directly or indirectly dependent on claim 12. Therefore, Appellant respectfully submits that Kaliski does not anticipate claims 13-18 for at least that reason.

B. Lenstra does not anticipate claims 19-24

i. Claim 19

Claim 19 is directed to a method for generating a basis independent bit string for use as a shared secret, in a cryptographic system. The method recites the following steps:

a) representing a first field element in terms of a first basis;

b) computing a first function of a first sequence of traces of said first field element; and

c) using said first sequence of traces as said bit string for performing cryptographic operations.

[identifiers added to the above for discussion purposes only]

ii. Lenstra

Lenstra teaches cryptosystems wherein participants select their own elliptic curve and finite field rather than using a centrally chosen elliptic curve. The curve is chosen from a predetermined set of curves. The public key is based on a participant's unique ID, which must be exchanged during communication setup for non-cryptographic reasons; and a randomly chosen bitstring having a length based on security considerations.

Figure 5 of Lenstra shows a flow chart for participant setup, and illustrates how a participant obtains part of its public key. The Examiner relies on Figure 5 and its description in columns 6 and 7. In Figure 5, the participant's cryptosystem selects values for various security parameters, and then randomly selects a bitstring having the same number of bits as one of the security parameters, i.e. Bs. The cryptosystem then obtains two integers by applying mapping functions to a concatenation of the participant's identity ID and the bitstring.

iii. Appellant's submissions regarding claim 19

The Examiner has stated, in part, that "[a]t step 515, the participant's cryptosystem randomly selects a bitstring s having Bs bits, that is for 'computing a first function of a first sequence of traces of said first field element'". However, the Examiner does not explain where Lenstra actually teaches the randomly selected bitstring being used for computing a first function of a first sequence of traces of a first field element.

In the response dated November 22, 2004, the Appellant argued that Lenstra does not disclose "computing a first function of a first sequence of traces of said first field element."

Appellant respectfully maintains this argument, with additional support as follows.

As noted above, Lenstra teaches a cryptosystem randomly selecting a bitstring to use in obtaining a pair of integers for generating part of its public key. The random bitstring is selected to have a length that corresponds to the length of a certain security parameter. This does not equal generating a basis independent bit string for use as a shared secret. This teaches randomly selecting a bitstring for use in obtaining part of a public key. The Appellant believes that the Examiner has misconstrued the teachings of Lenstra, and has improperly applied Lenstra in finding anticipation.

Referring to the above steps of claim 19, step a) requires that a first field element is represented in terms of a first basis. The method taught by Lenstra does not include such a step. The Examiner refers to Figure 5, yet the description accompanying Figure 5 does not show or even suggest a field element or a basis representation therefor, let alone the step of representing a first field element in terms of a first basis.

Regarding step b), the Examiner believes that Lenstra teaches such a step because Lenstra teaches generating a random bitstring. The Appellant respectfully disagrees. Firstly, step b) of claim 19 requires computing a first function <u>of a first sequence of traces</u> of said field element. Lenstra does not teach or even suggest the concept of a trace, let alone computing a first function of a first sequence of traces of the field element. It is unclear how the Examiner has come to this conclusion. The Appellant believes that it would involve a substantial leap of logic to contend that a randomly selected bitstring implies computing a first function of a first sequence of traces as recited in step b).

As described above, anticipation cannot be predicated on teachings in a reference that are vague or based on conjecture. In this case, the reference is not only vague in this regard, but in fact fails to even mention the concept of a trace.

The Appellant's have previously argued that a trace is a well defined concept and is described in the present application at paragraph 20. Claim 19 involves using a sequence of

traces as a bit string for use as a shared secret. Lenstra does not teach this or even suggest the use of such a concept. Therefore, Lenstra clearly cannot anticipate claim 19.

In view of the foregoing, the Appellant respectfully submits that Lenstra cannot serve as an anticipatory reference as it fails to even teach a single step of Appellant's claim 19.

iv. Appellant's submissions regarding claims 20-24

Claims 20-24 are either directly or indirectly dependent on claim 19. Therefore, Appellant respectfully submits that Lenstra does not anticipate claims 20-24 for at least that reason.

C. Claims 25-27 are patentable over the combination of Lenstra and Kaliski

i. Statement of the Law regarding patentability under 35 U.S.C. 103

According to section 2143 MPEP, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in the applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

ii. Claims 25-27

Claims 25-27 are ultimately dependent on independent claim 19. Claim 25 further defines the first function recited in claim 19 as being an irreducible polynomial of degree N.

Claim 26 further defines the second function recited in claim 20 (dependent on claim 19) as being an irreducible polynomial of degree N. Claim 27 is dependent on either claim 24 or 25, and recites, *inter alia*: "...said first field element is converted in terms of said second basis by finding a root for said polynomial for said first basis in a representation generated by said second basis; and evaluating said polynomial representing said first field element in said first basis at said root."

iii. Kaliski does not teach what is missing from Lenstra

The Examiner has applied the combination of Lenstra and Kaliski, since the Examiner has determined that Lenstra does not teach what is recited in claims 25-27.

The Appellant has discussed at length above that Lenstra does not teach any of the steps of claim 19, and is believed to have been improperly cited as an anticipatory reference therefor. Therefore, Kaliski, must at least not only teach what is missing from Lenstra, but also the additional features of claims 25-27 in order for the combination to be considered an obvious equivalent thereto.

The Appellant respectfully submits that a) the combination of Lenstra and Kaliski does not teach all elements in claim 19, b) Kaliski does not teach the elements introduced in claims 25-27, and c) there is no suggestion or motivation to even make the combination of Kaliski and Lenstra.

iv. Appellant's submissions

a) The combination of Lenstra and Kaliski does not teach all elements in claim 19

The Appellant's believe that Lenstra does not teach any of the steps recited in claim 19, outlined above. Therefore, Kaliski would need to teach all steps recited in claim 19. The teachings of Kaliski are summarized above. To briefly reiterate, Kaliski teaches various efficient methods and apparatus for basis conversion. Kaliski is not concerned with computing functions

of a sequence of traces of a field element, and is in fact entirely silent in that regard. Clearly, Kaliski does not teach any of the subject matter of claim 19. Accordingly, it is submitted that the combination of Lenstra and Kaliski does not teach every element of claim 19. Therefore, for at least this reason, claims 25-27 which are dependent upon claim 19 are patentable over the combination of Lenstra and Kaliski.

b) Kaliski does not teach the elements introduced in claims 25-27

The subject matter of claims 25-27 is summarized above. The Examiner relies on column 2, lines 17-32 and column 6, lines 1-5 of Kaliski as teaching the subject matter of claims 25-27. In column 2, Kaliski describes a polynomial basis representation having basis elements that are successive powers of γ. Kaliski further states that the polynomial f must be irreducible over the ground field GF(q). Claims 25-27 define the functions recited in claims 19 and 20 as being an irreducible polynomial of degree N. Although Kaliski refers to an irreducible basis polynomial, there is no reference to such polynomial being a function of a first sequence of traces of a field element. Similarly, the passage in column 6 relied on by the Examiner does not teach such a feature.

The Appellant believes the Examiner has relied on the benefit of 20/20 hindsight based on the Appellant's disclosure. Kaliski does not teach a function of a sequence of traces of a field element being a polynomial of degree N. Therefore, it is respectfully submitted that Kaliski does not teach the additional subject matter introduced in claims 25-27.

c) There exists no suggestion or motivation to combine Lenstra and Kaliski

The Examiner has stated that the ordinary skilled person would have been motivated to include the polynomial basis representation as in Lenstra's cryptosystem for a variety of reasons. The Examiner points to column 1, lines 25-28 of Kaliski. In this passage, Kaliski explains that for the purposes of cost, performance, etc. implementations of $GF(2^m)$ vary in their choice of basis.

The above statement by Kaliski generally describes the need to choose the most

appropriate basis representation for representing elements in a finite field. Kaliski is concerned with providing an efficient basis conversion apparatus and algorithm. Lenstra is concerned with providing users with a choice of their own elliptic curve and finite field. The Appellant believes that these motivations are divergent and that a person skilled in the art would not consider these references together for at least that reason.

Accordingly, the Appellant respectfully submits that neither Kaliski nor Lenstra, alone or in combination teach every element of claims 25-27, let alone independent claim 19, from which the claims depend. It is also submitted that there exists no motivation to combine Kaliski and Lenstra. Therefore, it is submitted that the Appellant's claims 25-27 clearly and patentably distinguish over the combination of Kaliski and Lenstra.

D. Claims 1-11 are patentable over the combination of Kaliski, Clapp, and Lenstra

i. Claim 1

Claim 1 is directed to a method for basis conversion between a pair of correspondents exchanging cryptographic data. The method recites the following steps:

a) transmitting an element represented in a first basis from a first correspondent to an intermediate processor;
b) converting the transmitted element into a second basis representation by said intermediate processor to produce a converted element;
c) forwarding said converted element to the first correspondent; and
d) operating on said converted element by said first correspondent in a cryptographic operation to obtain a result of said cryptographic operation for use in exchanging cryptographic data with a second correspondent.

[identifiers added to the above for discussion purposes only]

Steps a) to c) above are similar to certain steps recited in claim 12 that were described in detail above and argued with respect to Kaliski. In claim 1, an element represented in a first

basis is transmitted from a first correspondent to an intermediate processor similar to step a) of claim 12. Step b) of claim 1 is similar to step d) of claim 12, and step c) of claim 1 is similar to steps e) and f) of claim 12. Step d) involves the first correspondent operating on the converted element in a cryptographic operation for use in exchanging data with a second correspondent.

ii. Clapp

Clapp teaches public key cryptographic exchange methods using modular exponentiation. The method involves using memory for storing pre-computed results that can be flexibly traded off against the computational complexity of key-exchange. Although Clapp does generally describe cryptographic key exchange as indicated by the Examiner, Clapp does not teach or even suggest basis conversion, let alone basis conversion using an intermediate processor.

iii. The Appellant's submissions regarding claim 1

Firstly, as indicated above, claim 12 was argued with respect to Kaliski. Steps a) to c) of claim 1 are similar to steps recited in claim 12. Therefore, the arguments made with respect to claim 12, equally apply to claim 1. The Appellant notes, however, that the Examiner states, in part, "...Kaliski does not explicitly explain in great detail of how Kaliski's cryptographic processor supports cryptographic operations in multiple bases." This entirely contradicts the Examiner's position regarding claim 12, in which the Examiner states that Kaliski teaches conversion in multiple bases. This further evidences that applying Kaliski in rejecting either claim 12 or claim 1 is inappropriate, and that the Examiner has not fully appreciated the teachings of the prior art that has been relied upon.

Secondly, the teachings of Lenstra have been outlined in great detail above, with respect to claims 19-27. The Appellant respectfully submits that the teachings of Lenstra do not refer to a first correspondent transmitting elements to an intermediate processor, and having the intermediate processor convert the element into a second basis representation, and then forward the converted element back to the correspondent for use in cryptographic exchange with a second correspondent. The Examiner has stated that Lenstra teaches generally, the exchange of

cryptographic keys between two cryptographic units. However, the Examiner has failed to identify where Lenstra teaches using an intermediate processor for basis conversion.

Thirdly, as noted above, Clapp does not teach basis conversion, let alone basis conversion using an intermediate processor. Clapp is concerned with an entirely different cryptographic operation, namely modular exponentiation for pre-computing results to save computational power.

Accordingly, none of Kaliski, Lenstra, nor Clapp, alone or in combination teach, nor even suggest, using an intermediate processor for basis conversion as recited in claim 1. Therefore, for at least that reason, claim 1 is believed to be patentable over the combination relied on by the Examiner.

Moreover, the Appellant believes that there exists no motivation in the references to make such a combination. For instance, Kaliski is concerned purely with efficient basis conversion; whilst Clapp is concerned with modular exponentiation, and does not even suggest that this method is applicable to basis conversion. The Appellants believe that the Examiner has relied on 20/20 hindsight, and the seemingly random combination of concepts found in the references.

In view of the foregoing, the Appellant respectfully submits that none of the references applied by the Examiner in rejecting claim 1 teach every element of the claim, and there exists no motivation to combine the references. Accordingly, it is submitted that claim 1 is clearly and patentably distinguished over the combination of Kaliski, Lenstra and Clapp.

iv. <u>The Appellant's submissions regarding claims 2-11</u>

Claims 2-11 are either directly or indirectly dependent on claim 1, and as such for at least that reason, are also believed to distinguish over the combination of Kaliski, Lenstra and Clapp.

XI. CONCLUSION

Firstly, the Examiner has erred in finding that claims 12-18 are anticipated by Kaliski, when this reference fails to teach every element of the claimed invention.

Secondly, the Examiner has erred in finding that claims 19-24 are anticipated by Lenstra, when this reference fails to teach any of the steps recited in the claimed invention.

Thirdly, the Examiner has erred in finding that claims 25-27 are unpatentable in view of the combination of Lenstra and Kaliski. Lenstra fails to teach every element of claim 19, from which claims 25-27 ultimately depend. Moreover, Kaliski fails to teach the elements missing from Lenstra, fails to teach the subject matter introduced by claims 25-27, and there exists no motivation to combine Lenstra and Kaliski.

Finally, the Examiner has erred in finding that claims 1-11 are unpatentable in view of the combination of Kaliski, Lenstra and Clapp. None of these references, alone or in combination teach every element of the invention claimed in claims 1-11. Moreover, there exists no motivation to combine these references, and the Examiner's position, in part, contradicts the position taken regarding claim 12.

In view of the foregoing, the Appellant respectfully submits that claims 1-27 are clearly and patentably distinguished over the prior art cited by the Examiner and are in condition for allowance.

Therefore, the Appellant respectfully requests that this honorable Board of Patent Appeals and Interferences reverse the Examiner's decision in this case and indicate the allowability of claims 1-27 in this application.

Respectfully submitted,

John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: September 29, 2005

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/BSL

APPENDIX A

Listing of claims under appeal:

1. A method for basis conversion between a pair of correspondents exchanging cryptographic data, said method comprising the steps of:

transmitting an element represented in a first basis from a first correspondent to an intermediate processor;

converting the transmitted element into a second basis representation by said intermediate processor to produce a converted element;

forwarding said converted element to the first correspondent; and

operating on said converted element by said first correspondent in a cryptographic operation to obtain a result of said cryptographic operation for use in exchanging cryptographic data with a second correspondent.

2. A method according to claim 1 further comprising the step of: transmitting the result of said cryptographic operation to said second correspondent.

3. A method according to claim 2, wherein said result is a signature.

4. A method according to claim 2 further comprising the step of transmitting said converted element by said intermediate processor to said second correspondent.

5. A method according to claim 2 further comprising the step of transmitting said converted element by said first correspondent to said second correspondent.

6. A method according to claims 4 and 5, wherein said converted element is a short term public key.

7. A method according to claims 4 and 5, wherein said converted element is a long term public key.

8. A method according to claim 1, wherein at least one of said correspondents is a low power computing device.

9. A method according to claim 8, wherein said low power computing device is a smartcard.

10. A method according to claim 1, wherein said cryptographic operation employs an elliptic curved scheme.

11. A method according to claim 1, wherein said intermediate processor is a Certifying Authority.

12. A method for information exchange between a pair of correspondents exchanging cryptographic data and operating in different bases, the method comprising the steps of:

transmitting an element represented in a first basis from a first correspondent to an intermediate processor;

transmitting a second element represented in a second basis from a second correspondent to said intermediate processor;

converting the transmitted first element into said second basis representation by said intermediate processor to produce a first converted element;

converting the transmitted second element into a first basis representation by said intermediate processor to produce a second converted element;

forwarding said first converted element to said second correspondent; and

forwarding said second converted element to said first correspondent.

13. A method according to claim 12 further comprising the step of operating on said second converted element by said first correspondent in a cryptographic operation to produce a result.

14. A method according to claim 13 further comprising the step of operating on said first converted element by said second correspondent in said cryptographic operation to produce a second result.

15. A method according to claims 13 and 14, wherein said converted elements are public keys.

16. A method according to claim 15, wherein said result is a common key shared between said correspondents.

17. A method according to claim 16 further comprising the step of employing said common key in subsequent steps of a cryptographic scheme.

18. A method according to claim 17, wherein said cryptographic scheme is an elliptic curve scheme.

19. In a cryptographic system, a method for generating a basis independent bit string for use as a shared secret, the method comprising the steps of:

representing a first field element in terms of a first basis;

computing a first function of a first sequence of traces of said first field element; and

using said first sequence of traces as said bit string for performing cryptographic operations.

20. A method according to claim 19 further comprising the steps of:

representing a second field element in terms of a second basis; computing a second function of a second sequence of traces of said second field element; and

using said second sequence of traces as said bit string.

21. A method according to claim 20, wherein said first function is equal to said second function.

22. A method according to claim 20, wherein an order of said sequence of traces is shared between a first correspondent and a second correspondent.

23. A method according to claim 20 further including the step of using said bit string as a shared secret in a cryptographic scheme between a first correspondent and a second correspondent.

24. A method according to claim 23, wherein said cryptographic scheme is an elliptic curved scheme.

25. A method according to claim 19, wherein said first function is an irreducible polynomial of degree N.

26. A method according to claim 20, wherein said second function is an irreducible polynomial of degree N.

27. A method according to claims 24 and 25, wherein said first field element is converted in terms of said second basis by finding a root for said polynomial for said first basis in a representation generated by said second basis; and evaluating said polynomial representing said first field element in said first basis at said root.

21443858.1